

[TRANSLATION]

Korean Laid-Open Patent Publication No.10-2004-0072447 (August 18, 2004)

(19) KOREAN INTELLECTUAL PROPERTY OFFICE (KR)
(12) PATENT APPLICATION GAZETTE (A)

(51) Int. Cl.⁷

G06F 17/60A2

(11) Publication No. 10-2004-0072447

(43) Publication Date: August 18, 2004

(21) Application No.: 10-2003-0008929

(22) Filing Date: February 12, 2003

(71) Applicant(s):

CHUNG EUN YOUNG [KR]

(72) Inventor(s):

CHUNG EUN YOUNG [KR]

(74) Attorney(s)

AJU Patent & Law Firm

Request for Examination: filed

(54) Title of Invention: System and Method for Banking Security Using Mobile Terminal Linked with Account/Amount

Fig. 3 is a block schematic diagram which shows the constitution of mobile communication switch applied to the banking security system using mobile terminal linked with account/amount according to Embodiment 1 of the present invention.

Referring to this, the mobile switching center (16) applied to the banking security system using mobile terminal linked with account/amount comprises a plurality of connection switching section (50A, 50B), network connection module (62), number translation processor (54), SMS processing processor (56), code processing processor (58), data link processor (60), central control module (66) and information storing section (68). Furthermore, the mobile switching center (16) is connected with an authentication center (70: AUC) to process an authentication as to whether each of the mobile terminals is used legally.

In the above figure, the plurality of connection switching section (50A, 50B) processes calls generated from the mobile terminals (HP1, HP2) via the mobile communication base station (10A, 10B), mobile communication relay station (12A, 12B) and mobile

communication control station (14) and implements a data interface for transmitting an additional use approval request information of the card to the mobile terminals (HP1, HP2) upon receiving the use approval request information of the card by connecting with the VAN company server (17) and the banking servers (18A~18N).

The network connection module (62) forms the call passage of mobile terminal by number translation of mobile communication terminal, and is provided to receive the information of set/release of lock of account for the use approval of the card.

Furthermore, the number translation processor (54) performs the number translation for searching for the account linked with the corresponding mobile terminals (HP1, HP2) by interpreting the information for set/release of lock of account received from the mobile terminal and the number of the mobile terminal. The SMS processing processor (56) performs the SMS generation processing for querying to a user by writing SMS with information for use approval request of the card received from the VAN company server (17) and the banking servers (18A~18N).

Meanwhile, the code processing processor (58) performs the processing the corresponding code with the number of mobile terminal by receiving code data for set/release of the lock of account from the mobile terminals (HP1, HP2).

In the above figure, the data link processor (60) is linked with the VAN company server (17) and the banking servers (18A~18N) to perform the data link for the VAN company server (17) and the banking servers (18A~18N) and the data link processing for user's account in order to receive the use approval request information of the card.

The central control module (66), which is provided to control various functions associated with the call connection including the call passage set of the network connection module (62) and data transmission/receipt, recognizes the code information transmitted from the mobile terminal in which set/release of lock of account is implemented and the number of the mobile terminal, stores them in the information storing section (68), sets or releases the lock of optionally corresponding account and transmits the information to the VAN company server (17) and the banking servers (18A~18N).

The information storing section (68) stores account information for users at the same time of storing the input code information transmitted from the mobile terminal in which set/release of lock of account is implemented and stores the text message for use

approval request information of the card from the VAN company server (17) and the banking servers (18A-18N).

(57) THE CLAIMS

1. A banking security system using a mobile terminal linked with account/amount, the banking security system comprising:

a first approval means for, when a use approval request signal is generated from an ATM or a card settlement terminal in an affiliate, generating an approval signal by implementing an authentication of the corresponding card, the first approval means including a banking server or a VAN company server;

a second approval means for generating an approval acceptance/rejection signal for the corresponding card or account upon receipt of SMS for the approval acceptance/rejection by using a mobile terminal to generate an approval acceptance/rejection signal for an account or card set by a user;

an approval set means for allowing a use of account or card by registering an account or card that a user designates in advance via the second approval means, by implementing a set/release of lock of the account or card designated via the second approval means, when receiving the use signal of the card or account from the first approval means, by transmitting a SMS of query data on the corresponding use approval acceptance/rejection to the second approval means in case of the card or account for which the lock is set, and by transmitting the received response data thereon to the first approval means; and

a data relay means for implementing a transmission/receipt of various data, the data relay means including a mobile communication base station, mobile communication relay station and mobile communication control station mediated among the first approval means, the second approval means and the approval set means.

2. The banking security system using a mobile terminal linked with account/amount according to Claim 1, wherein the second approval means includes:

a plurality of function key buttons for inputting a telephone number of an opposite party according to a selection operation of a user and for selecting various menu functions for selecting a card and a use approval thereof, the function key buttons provided to write code information for the use approval of the corresponding card by performing the selection key inputs for the SMS regarding the transmitted use approval request of a card;

a key input section comprising a mode set key button for implementing a lock set

mode for a use approval of a card, a registration key button which is also used as # button for registering a set/ release of lock and in the corresponding lock set mode, up/down key buttons for selecting an account displayed on the display section and a lock set/release menu, and numeric key buttons for inputting a password in the lock set/release;

a display section for displaying visually an output of an account number and bank information according to the function operation status of the key input section and the display status or the selection status of the lock set/release mode and for displaying visually the approval request message for the card use transmitted from the mobile communication switch, the display section including a display means of film type such as a liquid crystal display device;

a duplexer for separating the transmitted/received signals by performing a wire communication with a base station of mobile communication network via the antenna;

a receiving section for receiving a voice signal or text information from a mobile terminal, a wire telephone terminal or a mobile communication switch of the opposite party via the antenna and the duplexer;

a receiving section for receiving a voice signal or text information from a mobile communication terminal, wire telephone terminal or mobile communication switch of an opposite party via the antenna and the duplexer;

a transmitting section for filtering and amplifying the voice signal input from the microphone and the code information set according to the lock set/release mode of account so as to be able to be transmitted;

a voice processing section for signal processing the voice signal received from the opposite party via the receiving section to be output through the speaker and for signal processing the voice signal of a user input from the microphone to be output to the transmitting section;

a memory linked with the processor for a lock set/release of account, wherein code data on account information for a lock set of account and code information table on selection information for a lock set/release of account are stored; and

a control section for writing the code information for a lock set/release of account selected by the key input section through the code information table from the memory and transmitting the code information to a remote server under the implementation of a lock set/release mode of account by the key operation of the key input section.

3. The banking security system using a mobile terminal linked with account/amount according to Claim 1, wherein the approval set means includes:

an authentication center for authentication processing a legal use of each of the mobile terminals;

a connection switch connected to the VAN company server and the banking server for processing each of calls generated from the mobile terminals via the mobile communication base station, mobile communication relay station and mobile communication control station and for performing data interface to transmit an additional approval request information of card use to the mobile terminals upon receipt of approval request information of card use;

a network connection module for forming a call passage of mobile terminal by the number translation of mobile communication terminal and for receiving the lock set/release information of account for the approval of the card use;

a number translation processor for performing the number translation to search for an account linked with the corresponding mobile terminal by interpreting information on the lock set/release of account received from the mobile terminal and the number of the mobile terminal;

a SMS processing processor for performing a SMS generation processing to quire to a user by writing a SMS with information on the approval request of card use received from the VAN company server and banking server;

a cord processing processor for processing the corresponding code together with the number of mobile terminal after being provided code data for lock set/release of account from the mobile terminal;

a data link processor for performing a data link for the VAN company server and banking server and a data link processing for an account of each of users in order to receive the approval request information of card use by connecting to the VAN company server and banking server;

a central control module for controlling various functions relating to a call connection comprising a call passage set of the network connection module and a transmission/receipt of data, the central control module being provided to recognize code information transmitted from the mobile terminal by which a lock set/release of account is set and the number of the mobile terminal, to store the information in the storage section, to set or to release the lock for the selective corresponding account and to transmit the information to the VAN company server and banking server; and

a information storing section for storing account information of each of users at the same time of storing the input code information transmitted from the mobile terminal by which a lock set/release of account is performed and for storing a text message for an approval request information of card use from the VAN company server and banking server.

4. The banking security system using a mobile terminal linked with account/amount according to Claim 1, wherein the first approval means includes:

an interface section for transmitting a SMS of approval information of card use for the mobile terminal by connecting to the approval setting means and for performing data interface to receive code information on an approval of card use from the mobile terminal;

a connection module for transmitting/receiving various data relating to an approval of card use by performing a connection with the approval setting means by the interface section as a medium;

a code interpretation processor for writing/transmitting code information on an approval of card use to the mobile terminal and for interpreting a code for the approval of card use applied from the corresponding mobile terminal;

a lock setting processor for performing a lock set/release of account according to the code interpretation of approval of card use which is interpreted in the code interpretation processor regarding the registered account or card of a user;

a SMS generating processor for writing a text message for transmitting the information to the corresponding mobile terminal of a user upon receiving an approval request signal for card use from an ATM terminal or VAN company server;

an account management processor for classifying and managing a plurality of accounts or cards which a user registers and for performing a management for a use approval of account or card by linking to the lock setting processor;

a information storing section for storing the code information for use approval of card or account and the setting information of card or account set by a user, the information storing section being provided to store card or account information by the number of mobile terminal of each of users;

a central control module for sending a SMS for an approval request information of card use to a mobile terminal of a user who has the corresponding card upon receiving a card approval request signal generated from various terminals relating to card settlement (e.g., card settlement terminal in affiliates or ATM, etc.) and for performing an approval of card use upon receiving the response signal thereto.

5. The banking security system using a mobile terminal linked with account/amount according to Claim 4, wherein

the SMS for approval request of card use to the mobile terminal further includes a sending control packet data for automatically re-sending to the banking server according to the confirmation button operation of a user.

6. A banking security method using a mobile terminal linked with account/amount, said banking security method comprising:

linking the opened card or account of a specific user to a banking server or VAN

company server connected to a mobile communication switch by using a mobile terminal so as to allow a remote set of a lock of the card or account;

receiving a use approval request signal of card or account from the banking server or VAN company server;

the first approving for performing an authentication for the corresponding card or account;

requesting to the mobile communication switch the second use approval of the corresponding card or account;

determining whether a lock is set for the corresponding card or account;

if the lock is set, transmitting to the mobile terminal of the corresponding user a SMS as to whether to release the lock; and

generating the second approval signal by releasing the lock of the corresponding card or account using the mobile terminal by a user.

7. A banking security method using a mobile terminal linked with account/amount according to Claim 6, further comprising:

autonomously generating the second approval signal regardless of an approval of a user if the lock for the card or account of the corresponding user is not set in the mobile communication switch.

8. A banking security method using a mobile terminal linked with account/amount according to Claim 6, further comprising:

inputting a separate password different from the password of the card or account;

selecting the account or card for releasing the lock; and

selecting a menu for a lock set/release in the process of generating the second approval signal by releasing the lock of the corresponding card or account using the mobile terminal by a user.

9. A banking security method using a mobile terminal linked with account/amount according to Claim 6, further comprising:

releasing the lock for amount that can be withdrawn/used from the corresponding card or account using the mobile terminal by a user;

receiving the second approval request signal and the information of the use amount from the banking server or VAN company server;

determining whether the lock of the corresponding account or card is set; determining whether the corresponding use amount is larger than the amount that the lock is set; and

generating the second approval signal.

10. A banking security method using a mobile terminal linked with account/amount according to Claim 9, further comprising:

releasing the lock for daily use amount; and

performing the release by renewing the lock for the corresponding daily use amount every day in the process of releasing the lock for the use of the corresponding amount by setting a certain amount of the corresponding card or account using the mobile terminal by a user.

공개특허공보 제10-2004-0072447호(2004.08.18.) 1부.

10-2004-0072447

(19) 대한민국특허청(KR)

(12) 공개특허공보(A)

(51) Int. Cl.⁷
G06F 17/80A2(11) 공개번호 10-2004-0072447
(43) 공개일자 2004년08월18일

(21) 출원번호	10-2003-0006888
(22) 출원일자	2003년02월12일
(71) 출원인	정원현
(72) 발명자	서울특별시 강동구 문준동 176-1(18/2) 주공이피트 301-1003 정원현
(74) 대리인	서울특별시 강동구 문준동 176-1(18/2) 주공이피트 301-1003 특허법인 마우

실시예구: 없음

(54) 제목/글자 명칭형 모바일 단말기를 이용한 금융보안시스템 및 그 방법

요약

본 발명은 계좌/금액 인증형 모바일 단말기를 이용한 금융보안 시스템 및 그 방법에 관한 것으로, 특히 유저가 소지한 다수의 금융 계좌를 유저가 모바일 단말기를 이용하여 일회성 사용 연거불하게 자동 설정할 수 있도록 이동통신망과 금융서비스를 연계함으로써 카드를 통한 현금 및 현금서비스를 발급받지 않고도 현금 설정된 경우 현금 일괄 인출이 가능하게 한, 계좌/금액 인증형 모바일 단말기를 이용한 금융보안 시스템 및 그 방법을 제공한다. 그 목적이 있다.

본 발명은 금융서비스를 한시 서비스로 이루어져 ATM이나 거점점 카드결제 단말기로부터 사용승인 요구수령이 발생되면, 해당 카드의 인증을 수행하여 승인신호를 발생시키도록 하는 1차 승인수단과; 상기 1차 승인수단과 더불어, 유저가 설정한 계좌나 카드의 사용여부에 대한 승인신호를 발생시키기 위해 모바일 단말기를 이용하여 구성되며, 승인 여부에 대한 SMS를 전송받아 해당 카드나, 계좌에 대한 승인 거부신호를 발생시키는 2차 승인수단과; 상기 2차 승인수단을 통해 유저가 미리 지정된 계좌나 카드를 등록시키고, 2차 승인수단을 통해 지정된 계좌나 카드의 적금/예금잔액을 받아, 상기 1차 승인수단으로부터 카드나 계좌의 사용승인호를 접수받아 책 설정된 카드나 계좌의 경우 해당 사용승인 여부인 대입 잔액에대한 SMS를 2차 승인수단으로 전송하고, 그 동안 데이터를 수신하여 1차 승인수단으로 전송함으로써 계좌나 카드의 사용이 가능하도록 하는 승인 설정수단과; 상기 1차 승인수단, 2차 승인수단 및 승인 설정수단의 사이에 해가인 이동통신망, 이동통신 중계국, 이동통신 제어국으로 이루어진 적금 데이터의 송수신을 할하는 데이터 중계수단으로 이루어진 것을 특징으로 한다.

본 발명을 적용하면, 카드나 현금이나 도장을 도난당하거나 분실, 또는 카드의 불법복제시에도 금융서비스를 승인하는 방법으로 유저의 모바일 단말기에서 승인신호를 발생하도록 하여 복수개의 승인이 이루어질 경우에만 해당 계좌나 카드를 사용할 수 있도록 함으로써 금융보안 장치로 사용할 수 있다는 장점이 있으며, 유저의 설정에 따른 일괄 금액에 대해서는 복통 해지함으로써 별도의 승인없이 카드나 계좌를 사용할 수 있도록 함으로써 더욱 편리하게 사용할 수 있으며, 해당 복통 해제함으로써 승인 없이 사용할 수 있는 일괄금액이나 사용잔액 금액을 감소시킬 수 있으므로 보다 안전한 금융서비스를 이용할 수 있다는 효과가 있다.

도면도

도1

명세서

도면의 간단한 설명

도 1은 본 발명의 제 1 실시예에 따른 계좌/금액 인증형 모바일 단말기를 이용한 금융보안 시스템의 개략적인 구성을 도시한 도식도.

도 2는 본 발명의 제 1 실시예에 따른 계좌/금액 인증형 모바일 단말기를 이용한 금융보안 시스템에 적용된 모바일 단말기의 구성을 도시한 블록구성도.

도 3은 본 발명의 제 1 실시예에 따른 계좌/금액 인증형 모바일 단말기를 이용한 금융보안 시스템에 적용된 이동통신망의 구성을 도시한 블록구성도.

도 4는 본 발명의 제 1 실시예에 따른 계좌/금액 인증형 모바일 단말기를 이용한 금융보안 시스템에 적용된 금융서비스의 구성을 도시한 블록구성도.

도 5a, 5b는 본 발명의 제 1 실시예에 따른 계좌/금액 인증형 모바일 단말기를 이용한 금융보안 시스템의

10-2004-0072447

음료보안 설정화면을 도시한 도면.

도 9a, 9b, 9c는 본 발명의 제 1 실시예에 따른 제과/음료 연동형 모바일 단말기들 이용한 음료보안 시스템의 다른 음료보안 설정화면을 도시한 도면.

도 7은 본 발명의 제 1 실시예에 따른 제과/음료 연동형 모바일 단말기들 이용한 음료보안 시스템의 음료보안 설정화면을 도시한 블록도이다.

도 9a는 본 발명의 제 1 실시예에 따른 제과/음료 연동형 모바일 단말기들 이용한 음료보안 시스템의 신호 흐름 도시한 블록도이다.

도 9a, 9b는 본 발명의 제 2 실시예에 따른 제과/음료 연동형 모바일 단말기들 이용한 음료보안 시스템의 음료보안 설정화면을 도시한 도면.

도 10은 본 발명의 제 2 실시예에 따른 제과/음료 연동형 모바일 단말기들 이용한 음료보안 시스템의 신호 흐름 도시한 블록도이다.

도 11a, 11b는 본 발명의 제 3 실시예에 따른 제과/음료 연동형 모바일 단말기들 이용한 음료보안 시스템을 통해 음료보안 설정화면을 도시한 도면.

도 12는 본 발명의 제 3 실시예에 따른 제과/음료 연동형 모바일 단말기들 이용한 음료보안 시스템의 신호 흐름 도시한 블록도이다.

도면의 주요부분에 대한 부호의 설명

MP1, MP2: 모바일 단말기.

17: 랜 서버.

16: 이음통신 교환기.

18A~18N: 음성 서버.

발명의 실시예 설명

발명의 목적

본 발명이 속하는 기술분야 및 그 분야의 종래기술

본 발명은 제과/음료 연동형 모바일 단말기들 이용한 음료보안 시스템 및 그 방법에 관한 것으로, 보다 상세하게 특정 유치가 소지한 다수의 금융 계좌를 유치가 모바일 단말기를 이용하여 일괄적으로 사할 수 있게 하는 금융보안 시스템을 제공한다. 본 발명은 금융보안 시스템을 통해 금융보안 설정화면을 도시한 도면.

도 12는 본 발명의 제 3 실시예에 따른 제과/음료 연동형 모바일 단말기들 이용한 음료보안 시스템의 신호 흐름 도시한 블록도이다.

도면의 주요부분에 대한 부호의 설명

MP1, MP2: 모바일 단말기.

17: 랜 서버.

16: 이음통신 교환기.

18A~18N: 음성 서버.

발명의 실시예 설명

발명의 목적

본 발명이 속하는 기술분야 및 그 분야의 종래기술

본 발명은 제과/음료 연동형 모바일 단말기들 이용한 음료보안 시스템 및 그 방법에 관한 것으로, 보다 상세하게 특정 유치가 소지한 다수의 금융 계좌를 유치가 모바일 단말기를 이용하여 일괄적으로 사할 수 있게 하는 금융보안 시스템을 제공한다. 본 발명은 금융보안 시스템을 통해 금융보안 설정화면을 도시한 도면.

도 12는 본 발명의 제 3 실시예에 따른 제과/음료 연동형 모바일 단말기들 이용한 음료보안 시스템의 신호 흐름 도시한 블록도이다.

도면의 주요부분에 대한 부호의 설명

MP1, MP2: 모바일 단말기.

17: 랜 서버.

16: 이음통신 교환기.

18A~18N: 음성 서버.

10-2004-0372447

카드 사용을 허가해주는 방식이다

물론 유자의 모비일 단상기와 병도의 표본세상을 구비하지 않은 상태에서 카운다운 용인여부과 대한 조의문장이 포함된 유제 대의태에 대한 제언선화가 표방되게 하며 이종출신 교향기물부터 오비일 단상기로 교향기물로부터 유제가 카운다운을 대한 용인여부과 판적하게 되면 사실으로 해당 SMS 대의태가 마땅한 교향기물로서 유제와 병도 그 용인여부가 여주어지게 하는 방식이다.

이것은 유체가 움직여버니 댐서 서배에 무슨 힘(力)을 동해 접속하여 카드 사용여부에 대한 승인용 카드 사용 전 따라 지를하는 것으로, 움직여버니 댐서 서배는 그 카드사용에 대한 승인을 미리 지령하지 않은 카드에 대해 사용오류가 있어도 이를 승인하지 않도록 하는 방식으로 카드의 불법 사용을 방지하도록 하는 방식에 그 예로서 제시할 수 있다.

[illegible]

이들 위에, 본 발명의 제 1 실시예에 따른 지지/굴해 연결형 모방 및 단결기형 이형한 음향보완 시스템은 다수의 모방 및 단결기(HP1, HP2) 및, 다수의 이동음선 거울곡(10A, 10B), 이동음선 절곡곡(12A, 12B), 이동음선 제어곡(14) 및, 이동음선 곡절기(18), 변위 서보(17), 다수의 음향저항(38A~38E)로 구성된다.

● 모뎀에서, 송기 이송통신 기지국(10A, 10B)(Base Station Transceiver: BTS)은 송기 유체가 각각 유대하고 있는 모뎀을 연결함(HF1, HF2)의 이송위치 때문에 다수개가 분할적으로 설치되고서, 해당 모뎀의 송신기(HF1, HF2)가 이송위치에 송신통과 할 후선테이더의 전달/중복이 가능하도록 상태방목 여충을 단행하고 후선송출 경로를 송신할 수 있는 송신 송수신기를 송신할 수 있는 송신기(송수신기)를 단행함

설기 이득흥선 종가국(12A, 12B)을 설기 자의의 여흥종선 가자국(10A, 10B)과 설기 이득흥선 제미국(14) 간
을 종가하여 연결하기 위한 것이고, 설기 이득흥선 제미국(14)은 설기 격학의 이득흥선 종가국(12A, 12B)을
통하여 설기 이득흥선 가자국(70A, 10B)의 종말가능과, 각 가자국 집단간의 상호연계로, 사회적 재료를
수용하기 위한 것이다.

을 도면에서, 삼가 마형등신 교현가(16)는 삼가 오비형 단일가(HP1, HP2)가 정상적으로 동작 가능한 상태
에서, 다수의 가형질 결핵 단일가(도식 9)와도 접속될 수 있는 서브(17) 및 다수의 공용서브(18A~18K)와 동시
에 접속되어 기동측을 유제와 카드 사용으로 전송할 뱀사 선로(17) 및 공용서브(18A~18K)를 포함하여 연가
도록 되어 있으며, 그 카드 사용에 대한 승인 요구신호를 삼가 오비형 단일가(HP1, HP2)로 전송하여 그 때
연가도록된 통신선로 접속하여 뱀사 서브(17) 및 공용서브(18A~18K)로 전송함으로써 카드 사용에 대한 승인
연하도록 각종 승인신호에 대한 연가도록 승수를 행하는 수단이 다.

특, 도 1에 도시된 바와 같이, 본 발명의 실시예에서 생산 서버(17)는 음성저장부(18A~18G)에서 해당 카드로 대한 시동 인증을 행하는 음인검출에 대하여, 유직자 소지한 모바일 단말기(HP1, HP2...)를 이용한 음인검출을 추가적으로 수행할 수 있다. 이하, 모바일 단말기(HP1, HP2...)를 이용한 음인검출을 개략적으로 설명하면 다음과 같다.

0188. 为文和五世活佛(第1, 392...) 著 西藏佛教 五世达赖喇嘛 上列仁波切 传记 传记 传记

[illegible]

說得可驚動人之話以嚇得他離去。他離去時已滿五時。細砂

이들 식품종류에 대해 식품영양도 제 1차식사에 따른 계화/금화 연동형 오바일 단일가분 이음탄 함유비율 시스템에 적용된 모델값을 산출한 결과(HP2...)를 표 1과 같이 정리하였다. 표 1에서 HP2와 HP3의 경우, 탄수화물 함량이 높고 단백질 함량이 낮아 영양학적 관점에서 불합격으로 판정되었다. 반면 HP1은 탄수화물 함량이 적고 단백질 함량이 높으며, HP4는 탄수화물 함량이 적고 단백질 함량이 적으나 지방 함량이 높기 때문에 영양학적 관점에서 불합격으로 판정되었다. 한편 HP5는 탄수화물 함량이 적고 단백질 함량이 적으며, 지방 함량도 적어 영양학적 관점에서 합격으로 판정되었다.

본 논문에서, 삼기 귀환법(三起歸還法)은 사물자의 존재 조차와 미래 심대의를 변화시키는 일과, 문치해설자의 의도적 행위, 문치자, 일과, 카타르시스 및 사물성인물 위한 다양한 제반기능과 전략을 위한 다수의 기능적 의도적 구조가 있을 뿐, 전통적 카타르시스 승인인물과 대립하는 문치해설자에 대한 심대 귀환법을 행함으로써 새로운 카타르시스 승인인물 대립을 형성하는 것을 궁극적으로 지향하는 것으로 보인다.

[illegible]

여기서, 삼기 귀인(三歸)의 원(源)을 학계(學界)에서 대입(大入)한 것임에도 불구하고, 통속을 위한 계(階)로 일각 기는 여외(外)도, 편승(偏乘)의 양(量)에 따른 적(適)한 지(地)에서의 정(定)된 조(調)할 수 있도록 하(下)면 되고, 귀(歸)의 본(本)질(質)이 가(加)함(含)되어 있다.

[illegible]

10-2004-0072447

을 비정의 표시수단으로 이루어진다.

상기 표시부(22)는 상기 키입력부(20)의 모드설정키버튼에 키조작되어 개화, 선택 및 개화, 막 설정/해제, 8. 개화 막 설정, 4. 개화 막 해제 등의 설정을 위한 표시를 수행한다. 따라서, 각각의 숫자키를 일괄적으로 대는 한 메뉴를 선택할 수 있도록 한다.

도 2에서, 상기 디스플레이(28)는 상기 인터페이스(24)를 통해서 마우스클릭의 기저작과 무선충전을 수행하여 송/수신되는 신호를 분리하기 위한 것임이고, 상기 수신부(28)는 상기 인터페이스(24)와 유선/무선에서 통해서 송수신되는 이동통신 단말기나 무선충전 단말기 또는 이동통신 교환기(10)로부터의 송신신호 또는 충전정보를 수신함에 따라, 상기 수신부(28)는 상기 인터페이스(24)로부터의 입력된 송신신호 및 개화 막 설정/해제 모드에 따라 설정된 코드정보를 수신 가능하게 필터링 및 출력처리한다. 된다.

또한, 상기 음성 처리부(30)는 상기 수신부(28)를 통해서 수신받은 송신신호로부터의 음성신호를 신호 처리하여 상기 스피커(34)를 통해 출력하도록 하고, 상기 마이크로폰(36)으로부터 입력받은 음성신호의 음성 신호를 신호 처리하여 상기 송신부(30)에 출력하게 된다.

상기 메모리(38)는 개화 막 설정을 위한 코드정보에 대한 코드데이터 및 개화 막 설정/해제설정용 위한 선택정보에 대한 코드정보 데이터들이 저장되어 있으며, 개화 막 설정/해제 설정을 위한 프로세서가 필요하도록 되어 있다. 상기 제어부(40)는 상기 기동력부(20)의 키조작에 의한 개화 막 설정/해제 설정모드로 실행하면서, 그 키입력부(20)에 의해 선택되는 개화 막 설정/해제설정에 대한 코드정보를 상기 메모리(38)로부터 코드정보 데이터들을 통해 작성하여 입력 서비스로 전송하도록 한다.

도 2은 본 발명의 제 1실시예에 따른 개화/음향 연출용 모바일 단말기를 이용한 공연모반 시스템에 적용된 이동통신 교환기의 구성을 도시한 블록구성도이다.

이를 참조하면, 본 발명의 제 1실시예에 따른 개화/음향 연출용 모바일 단말기를 이용한 공연모반 시스템에 적용된 이동통신 교환기(10)는 복수개의 음성 교환부(50A, 50B)와, 영상처리부(52), 번호변환 프로세서(54), SMS 처리 프로세서(56), 코드처리 프로세서(58), 대역폭 컨트롤러(60), 장래제어 유닛(62), 및 정보 저장부(64)를 구상한다. 또한, 상기 이동통신 교환기(10)는 사 모바일 단말기와 적정한 사용자부호인접 처리하기 위한 인증센터(70: AUC)와 연결되어 있다.

흥 도면에서, 상기 복수의 음성 교환부(50A, 50B)는 상기 이동통신 기지국(10A, 10B)과 이동통신 장치(12A, 12B), 및 이동통신 제어기(14)를 통해서 상기 모바일 단말기(H1, H2)로부터 각자 발생하는 호출 처리, 상기 랜서 서버(17) 및 음성서비스(18A~18B)와 연결되어 키드 사용 승인요구 정보를 접수하여 상기 모바일 단말기(H1, H2)로 후기적인 카드사용 승인요구 정보를 전송하기 위한 데이터 인터페이스를 수행한다.

상기 합성곱 모듈(62)은 이동통신 단말기의 번호변환에 의해 모바일 단말기의 정보 전송을 형성시켜 주며, 카드사용 승인에 대한 개화 막 설정/해제설정 정보를 전송하기 위한 접속 모듈이다.

또한, 상기 번호변환 프로세서(54)는 모바일 단말기로부터 전송받은 개화 막 설정/해제설정에 대한 정보 및 그 모바일 단말기의 번호를 해석함으로써 해당 모바일 단말기(H1, H2)와 연결된 개화막 데이터가 위치하는 정보저장부를 수행하기 위한 것이고, SMS 처리 프로세서(56)는 상기 랜서 서버(17) 및 음성서비스(18A~18B)로부터 전송받은 카드사용 승인요구에 대한 정보를 SMS로 작성하여 유무선에 출력하기 위한 SMS 생성 모듈을 수행하는 프로세서이다.

한편, 상기 코드처리 프로세서(58)는 상기 모바일 단말기(H1, H2)로부터 개화 막 설정/해제설정에 대한 코드데이터를 제공받아, 해당 코드를 모바일 단말기 번호와 함께 처리하는 프로세서이다.

흥 도면에서, 상기 데이터 전송 프로세서(60)는 상기 랜서 서버(17) 및 음성서비스(18A~18B)와 연결되어 키드 사용 승인요구 정보를 접수하기 위해 랜서 서버(17) 및 음성서비스(18A~18B)와 대한 데이터 전송 및 각 유제별 개화막에 대한 데이터 인증처리를 수행하는 프로세서이다.

상기 정보처리 모듈(66)은 상기 합성곱 모듈(62)의 출력으로 설정된 정보하는 호출 및 데이터 전송에 관한 다양한 기능들 제어하기 위한 것으로서, 개화 막 설정/해제설정용 행하는 모바일 단말기로부터 전송된 코드정보 및 그 모바일 단말기 번호를 인식하여 상기 정보 저장부(68)에 저장시키고, 선택된 해당 개화막에 대한 확률 설정하거나 해제하고 그 정보를 상기 랜서 서버(17) 및 음성서비스(18A~18B)로 전송하도록 한다.

상기 정보 저장부(68)는 개화 막 설정/해제설정용 행하는 모바일 단말기로부터 전송되는 코드정보를 입력하여 및 정보 처리부(54)에서, 각 유제별 개화정보를 저장하고, 랜서 서버(17) 및 음성서비스(18A~18B)로부터의 카드사용 승인요구 정보에 대한 문자제시자를 제공할 있다.

도 2은 본 발명의 제 1실시예에 따른 개화/음향 연출용 모바일 단말기를 이용한 공연모반 시스템에 적용된 이동통신 교환기의 구성을 도시한 블록구성도이다.

이를 참조하면, 본 발명의 제 1실시예에 따른 개화/음향 연출용 모바일 단말기를 이용한 공연모반 시스템에 적용된 이동통신 교환기(10)는 복수개의 음성 교환부(50A, 50B)와, 영상처리부(52), 번호변환 프로세서(54), SMS 처리 프로세서(56), 코드처리 프로세서(58), 대역폭 컨트롤러(60), 장래제어 유닛(62), 및 정보 저장부(64)를 구상한다. 또한, 상기 이동통신 교환기(10)는 사 모바일 단말기와 적정한 사용자부호인접 처리하기 위한 인증센터(70: AUC)와 연결되어 있다.

한편, 본 발명에서는 그 일례인 카드 사용승인에 대한 데이터처리 작성 기능 및 그 결과정보 전송, 정보 정보 전송처리를 행하는 상기 음성서비스(18A~18B)에 대해 기술한다. 상기 랜서 서버(17)도 동일한 구성을 이루며 각 유제별 기능들 수행할 수 있으므로 이에 대한 설명은 생략하게 한다.

상기 음성서비스(18A~18B)는 그 내부에 인터페이스부(72), 인증센터(74: AUC), 접속유닛(76), 코드처리 프로세서(80), 확률 설정 프로세서(82), SMS 설정 프로세서(84), 개화 관리 프로세서(86), 데이터처리부(88),

1D-2004-0072447

정보 저장부(78)로 구성된다.

상기 인터페이스부(72)는 상기 이종통신 교환기(16)에 접속되어 모바일 단말기(HP1, HP2)에 대한 카드 사용 승인정보와 SWS를 전송하며, 그 모바일 단말기 (HP1, HP2)로부터 카드 사용 승인에 대한 코드정보를 수신하기 위한 데이터 인터페이스를 수행하는 수단이다.

상기 접속부(76)는 상기 인터페이스부(72)를 매개하여 이종통신 교환기 (16)와의 접속을 수행함으로써 카드 사용 승인관련 데이터를 송수신하기 위한 수단이며, 코드에서 프로세서(80)는 상기 모바일 단말기(HP1, HP2)로 카드 사용 승인에 대한 코드정보를 전송하며, 매칭 코드를 전달기(HP1, HP2)로부터 전달된 카드를 사용 승인에 대한 코드를 판독하기 위한 수단이다.

상기 칩 설정 프로세서(82)는 기동특성 유류의 제어나 카드정보에 대해 상기 코드에서 프로세서(80)에서 행한 카드 사용승인의 코드해석에 따라 자료 및 설정 및 그 해제를 실행하기 위한 수단이다.

상기 SWS 설정 프로세서(84)는 ATM 단말기(도시 생략)나 뎀서 서버(17)로부터 카드 사용에 대한 승인요구 신호가 접수되면, 그 정보에 따라 유류의 상태를 단말기(HP1, HP2)로 전송하기 위한 장치까지를 접속하는 수단이다. 이때, 카드 사용 승인요구에 대한 SWS 내에는 유류의 확인번호 코드에 따라 상기 금융서버(18A~18N)를 재발송하는 발송 제어 데이터가 더 포함되어 있는 것이 바람직하다. 따라서, 유류가 카드 사용 승인을 위한 카드를 발급하는 카드 코드를 판독하고, 확인번호만을 추적하게 되면 자금유출을 방지(18A~18N)로 전송하도록 할 수 있다.

상기 거래 정보 프로세서(86)는 유류가 등록된 다수의 거래 또는 카드를 각 유류별로 분류하여 관리하며, 상기 각 설정 프로세서(82)의 연동되어 거래나 카드의 사용 승인에 대한 관리를 행한다.

상기 정보 저장부(78)는 각 유류의 모바일 단말기 번호별 카드 또는 거래정보를 저장하고 있으며, 카드나 거래의 사용 승인에 대한 코드정보, 유류가 설정한 카드나 거래의 칩 설정정보를 저장하는 수단이며, 상기 정보 저장부(80)는 이들 카드출처 관련 단말기(도시 생략)가 발행 카드를 단말기나, ATM 코드로 발행 카드를 유류로 유입시킴으로써 유류가 카드 사용에 대한 승인요구 신호를 SWS로 전송하고, 그에 대한 응답신호를, 유류에 따라 카드 사용 승인을 통하는 수단이다.

대면대, 유류가 모바일 단말기(HP1, HP2)를 이용하여 카드나 계좌와 모바일 단말기(도시 생략)를 접속하는 카드 사용에 대한 승인요구 정보로 SWS를 이용하여 해당 유류의 모바일 단말기(HP1, HP2)로 전송한다. 해당 카드를 계좌에 칩을 설치하지 않은 상태에서는 카드 단말만을 상기 금융서버(18A~18N)나 뎀서 서버(17)에서 수행한 카드 사용 승인을 행하도록 한다.

도 5a, 5b는 본 발명의 제 1 실시예에 따른 거래/금액 연동형 모바일 단말기들 이용한 금융보안 시스템을 설명하기 위한 블록도이다.

이를 참조하면, 본 발명의 제 1 실시예에 따른 거래/금액 연동형 모바일 단말기들 이용한 금융보안 시스템은 상기 금융서버(18A~18N)나 뎀서 서버(17)에 연결되거나, 상기 금융서버(18A~18N)나 뎀서 서버(17)를 통하여 연결된 이종통신 교환기(16)에 대한 유류가 모바일 단말기(HP1, HP2)를 이용하여 특정 거래나 카드의 사용에 대한 칩을 발급하거나 해제를 할 수 있게 된다.

상기된 모바일 단말기(HP1, HP2)에는 별도의 거래 승인에 대한 퍼싱/해제 프로세서가 구비되어지고, 화면(80)을 통해 도 5a에 도시된 바와 같이 거래 확인/해제 모드로 출력시킬 수 있다. 그 거래 확인/해제 모드에는 1. 비밀번호 입력, 2. 계좌선택, 3. 거래 목적, 4. 거래 금액, 5. 거래 일자 등을 입력할 수 있다. 또한, 유류가 현재 잔액만을 출력하는 경우에도 이러한 코드에 응답하여 상기 금융서버(18A~18N)로 전송되거나, 상기 금융서버(18A~18N)나 뎀서 서버(17)로 전송되는 입력 번호이다.

따라서, 상기 금융서버(18A~18N)나 뎀서 서버(17)에서 해당 거래의 퍼싱 및 해제상태가 접수되면, 그에 따른 확인정보를 도 5b에 도시된 바와 같이 '○○○'의 거래 ××××××××××××의 금액/사유에 대한 칩(lock)이 설정되었습니다.'라는 단문 메시지가 전송되어 화면(82) 출력되게 된다.

즉, 카드를 도입받거나, 분실한 경우, 카드의 불법 해제가 있는 경우에는 유류가 미리 카드나 계좌에 칩을 설정한 상태라면, 해당 카드의 사용이 승인되지 않게 된다. 또한, 해당 카드나 계좌의 칩을 해제하기 위해서는 그 카드의 비밀번호를 입력한 상태만 비밀번호를 상기 모바일 단말기(HP1, HP2)에 입력하여야 하는 경우로 시스템은 파격이라 하였다. 도 5a, 5b에 도시된 화면은 카드 사용여부에 대한 승인 요구정보를 상기 금융서버(18A~18N)나 뎀서 서버(17)로부터 전송되지 않은 상태에서 유류가 모바일 단말기(HP1, HP2)로 입력하여 암호를 제어나 카드의 칩을 설정하고 해제하는 방식이다.

도 5a, 5b는 본 발명의 제 1 실시예에 따른 거래/금액 연동형 모바일 단말기들 이용한 금융보안 시스템의 다른 금융보안 설정화면을 도시한 도면이다.

이를 참조하면, 도 5a~5c에 도시된 방식은 카드 사용에 대한 승인요구신호가 상기 금융서버(18A~18N)나 뎀서 서버(17)로 전송되면, 그 카드 승인할 수 있고, 유류에게 2차 승인을 요구하기 위한 화면에 대해 도 5a에 도시된 것으로, 상기 금융서버(18A~18N)나 뎀서 서버(17)에서 확인된 SWS는 해당 유류의 모바일 단말기(HP1, HP2)로 전송되어 도 5a에 도시된 바와 같이 화면(84) 출력된다. 즉, '○○○'의 거래 ××××××××××××의 인증/사유 시도가 있습니다. 칩(lock)을 해제하시겠습니까? 라는 단문메시지가 출력된다. 그 화면에 '1. 예, 2. 아니오'를 숫자키 입력으로 선택하도록 되어 있다.

이 경우를 유류가 미리 특정 거래나 카드의 사용에 대한 칩을 설정한 상태로써, 만약 유류가 특정 거래나 카드 사용에 대한 칩을 설치하지 않은 상태라면 이러한 단문메시지는 전송되지 않는다.

대면대, 유류가 미리 본 발명으로부터 자신의 카드나 계좌를 사용하고 있는 것으로 판단하면, 2번을 선택하여 칩 설정상태를 유지하도록 할 수 있다. 그러면, 상기 금융서버(18A~18N)나 뎀서 서버(17)는 도 5b에 도시된 바와 같이 '○○○'의 거래 ××××××××××××의 칩 설정상태가 유지되어 인증/사유에 대해 승인되었으므로, 라는 단문메시지를 전송하여 화면(86) 출력되게 된다.

반면, 유류가 칩을 해제하는 1번을 선택한 경우라면, 도 5c에 도시된 바와 같이 상기 금융서버(18A~

10-2004-0072447

18N)나 뎀서 서버(17)는 도 8b에 도시된 바와 같이 '○○○'년의 계좌 xxx-xxx-xxx의 계좌이체 제의와 일치한다. 이는 단문메시지를 전송하여 회원(88)을 확인하는 것이다. 이때, 상기 금융서버(18A~18N)나 뎀서 서버(17)로부터 모바일 단말기(HP1, HP2)로 발송된 SMS에는 자동 재발송 제어 패킷 데이터가 내장되어 있으므로 유자가 재발송을 선택하고 확인받은 전송을 조작하면 자동 재발송 SMS는 상기 금융서버(18A~18N)나 뎀서 서버(17)로 재발송되지 않는다.

상기한 구성의 본 발명의 제 1 실시예에 따른 계좌/금액 전송용 모바일 단말기를 이용한 금융보안 시스템의 기동과 작동을 충분히 도면을 참조하여 상세하게 설명한다.

도 7은 본 발명의 제 1 실시예에 따른 계좌/금액 전송용 모바일 단말기를 이용한 금융보안 시스템의 금융보안 설정과정을 도시한 흐름도이다.

먼저, 유자가 모바일 단말기(HP1, HP2)를 이용하여 계좌의 발송정지 및 계좌정지등을 행하기 위해 계좌 연동 설정으로 들어 선택한다(제 1 단계: ST-1). 계좌 연동 설정으로 설정하기 위해서는 계좌 비밀번호와 일치한 모바일 단말기(HP1, HP2) 자체 비밀번호를 입력해야 한다(제 2 단계: ST-2).

비밀번호가 일치되면, 유자는 액 설정/해제설정을 위한 계좌를 선택하거나 입력한다(제 3 단계: ST-3). 계좌를 선택한 후 기능키를 누르면 액엔터, 액엔터로 조작한다(제 4 단계: ST-4). 그러면, 해당 모바일 단말기(HP1, HP2)에서는 계좌 전송을 위한 신호를 코드 데이터로 변환하여 이동통신 교환기(10)로 전송한다(제 5 단계: ST-5).

이에 따라, 이동통신 교환기(10)는 해당 계좌연동을 위한 코드데이터를 수신하고(제 6 단계: ST-6), 해당 금융서버(18A~18N)나 뎀서 서버(17)에 계좌 연동정보를 전송하여 해당 계좌 연동을 수행하도록 하고, 해당 계좌에 대한 발송정지 하도록 코드데이터를 작성한다(제 7 단계: ST-7). 코드데이터 작성에 완료되면, 뎀서 서버(17)는 해당 모바일 단말기(HP1, HP2)로 발송하여 회원에게 표시한다(제 8 단계: ST-8)(제 9 단계: ST-9).

도 8은 본 발명의 제 1 실시예에 따른 계좌/금액 전송용 모바일 단말기를 이용한 금융보안 시스템의 신호흐름을 도시한 흐름도이다.

먼저, 도 7에 도시된 바와 같이 모바일 단말기(HP1, HP2)를 이용한 계좌 연동 설정이 마무리된 상태에서, 유자가 그 모바일 단말기(HP1)를 이용하여 계좌를 찾아도 카나리상의 계좌를 검색할 수 있다. 이 경우, 유자는 액엔터, 액엔터로 조작한다(제 1 단계: ST-1). 그러면, 해당 모바일 단말기(HP1)는 액엔터, 액엔터로 조작한다(제 2 단계: ST-2). 그러면, 해당 모바일 단말기(HP1)는 액엔터, 액엔터로 조작한다(제 3 단계: ST-3).

그 상태에서, 해당 금융서버(18A~18N)나 뎀서 서버(17)로 ATM 단말기, 기밀번호 키로젝트 단말기 등을 통해 카드사용 신호가 접수되면, 상기 금융서버(18A~18N)나 뎀서 서버(17)는 상기 이동통신 교환기(10)로 카드 사용 승인요청신호를 전송한다.

그러면, 상기 이동통신 교환기(10)는 계좌 사용 승인요구에 대한 SMS를 작성하여, 해당 계좌의 '소지자인 유자의 모바일 단말기(HP1)'로 전송한다. 즉, 계좌나 카드의 사용에 대한 권한을 해당 유자에게 부여한다.

해당 점의 정보에 따라 유자가 액 설정을 유지하고자 하는 코드 신호를 발생시키면, 상기 이동통신 교환기(10)는 해당 계좌나 카드에 대한 작성된 유자시키고, 액을 해제하고자 하는 코드신호를 유자에게 발생시킨다. 유자가 이동통신 교환기(10)는 액을 해제시키고, 그 해제정보를 해당 금융서버(18A~18N)나 뎀서 서버(17)로 전송하여 승인신호를 발생시켜 카드나 계좌를 사용할 수 있도록 한다.

한편, 계좌나 카드 사용승인에 대한 SMS 정보는 이동통신 교환기(10)에서 작성하도록 할 수도 있으나, 상기 금융서버(18A~18N)나 뎀서 서버(17)에서 작성할 수 있으며, 이 경우 상기 이동통신 교환기(10)는 단순히 이러한 SMS 데이터의 송수신만을 행하도록 할 수 있다.

마지막, 본 발명의 제 2 실시예에 대해 도면을 참조하여 상세하게 설명한다.

도 8a, 8b는 본 발명의 제 2 실시예에 따른 계좌/금액 전송용 모바일 단말기를 이용한 금융보안 시스템의 금융보안 설정과정을 도시한 도면이다.

이들 참조하면, 본 발명의 제 2 실시예에 따른 계좌/금액 전송용 모바일 단말기를 이용한 금융보안 시스템은 유자가 모바일 단말기를 이용하여 소지한 다수의 신용카드에 계좌나 현금계좌, 가상계좌와 이통계좌와 일치하는 계좌를 검색할 수 있도록 이동통신서버와 금융서버를 연계함으로써 카드와 계좌를 동시에 검색하여 카드나 계좌로 이용한 금융 거래가 가능하게 하며 금융보안 및 보안에 관한 정보를 제공할 수 있도록 한다.

즉, 카드나 계좌의 사용여부에 대한 액을 설정하는 것과 마찬가지로, 본 발명에서는 카드나 계좌의 사용여부나 신용카드를 검색할 수 있는 액을 설정하여 그 액의 액에 대해서는 사용이나 신용이 불가능하도록 할 수 있는 방법을 제시한다.

이에 따라, 상기 모바일 단말기(HP1, HP2) 내부에는 카드나 계좌의 사용여부에 대한 액설정/해제설정을 위한 코드데이터를 생성시킬 수 있는 프로그램이 부가적으로 사용된다. 이 프로그램은 설정할 수 있도록 한다. 또한, 금융서버(18A~18N)나 뎀서 서버(17)에서 사용한다(제 1 단계: ST-1). 그러면, 해당 모바일 단말기(HP1, HP2)에서는 액엔터, 액엔터로 조작한다(제 2 단계: ST-2). 그러면, 해당 모바일 단말기(HP1, HP2)에서는 액엔터, 액엔터로 조작한다(제 3 단계: ST-3).

한편, 본 발명은 사용한다(제 4 단계: ST-4). 그러면, 해당 모바일 단말기(HP1, HP2)에서는 액엔터, 액엔터로 조작한다(제 5 단계: ST-5). 그러면, 해당 모바일 단말기(HP1, HP2)에서는 액엔터, 액엔터로 조작한다(제 6 단계: ST-6).

상기한 바와 같이 이루어진 시스템을 이용하여 유자는 모바일 단말기(HP1, HP2)를 통해 도 8a에 도시된 바와 같이, 1. 비밀번호 입력, 2. 계좌 검색에 이르게, 3. 액 해제정보 설정을 행할 수 있는 액(100)이 입력된다. 그 액(100)에서 유자가 액 해제정보를 입력하고, 액 해제나 카드로 선택한 후 액 해제정보를 입력하게 되면 해당 유자가 선택한 카드나 계좌의 사용여부 또는 액을 가능하게 설정한 금액으로 출력된다.

10-2004-0072447

다. 즉, 설정권책에 대해서는 약이 해제되게 되어 해당 금액만큼 승인여부를 종라하지 않고 사용할 수 있게 된다. 또한, 이 경우 설정권 금액은 신용카드사나 금융기관에서 사용자의 신용도에 따라 설정한 신용한도라는 의미이다.

즉, 해제금액이 설정되면, 상기 이통통신 교환기(16)는 해당 유자의 모바일 단말기(10)의 유자의 계좌 ×××-×××-×××××의 일 및 안(사용권도)에서 (10만원)에 약 해제금액입니다. 같은 SNS 데이터로 공유하여 회원(100) 등록시킴다.

상기한 유자의 본 발명의 제 3 실시예에 따른 계좌/금액 인증을 모바일 단말기를 이용한 금융보안 시스템의 기술적 적용을 확보한 도면을 참조하여 상세하게 설명한다.

도 10은 본 발명의 제 3 실시예에 따른 계좌/금액 인증을 모바일 단말기(10)를 이용한 금융보안 시스템의 신호 흐름을 도시한 블록도이다.

먼저, 유자가 그 모바일 단말기(10)를 이용하여 다수의 계좌와 관련된 하나 이상의 특정 계좌를 선택하여 이 선택에 기반한 계좌 인증 설정요구를 행한다. 상기 이통통신 교환기(16)는 해당 계좌에 대한 계좌 인증 설정을 행한다.

또한, 유자가 해당 계좌에 대해 특정 금액을 인증하여 해당 계좌의 사용한다 및 인증 가능금액에 대한 인증 설정을 요구한다. 상기 이통통신 교환기(16)는 해당 사용금액에 대한 약 설정 요구의 코드데이터를 수신하여 선택 계좌의 사용금액에 대한 작을 설정한다.

그 상태에서, 해당 금융서버(18A~18N)나 연사 서버(17)로 ATM 단말기, 가맹점 코드/결제 단말기 등을 통해 카드사 신용카드로 전송된다. 상기 금융서버(18A~18N)나 연사 서버(17)는 상기 이통통신 교환기(16)로 카드 사용 승인요구신호 및 승인금액의 정보를 전송한다.

그러면, 상기 이통통신 교환기(16)는 해당 계좌가 약 설정된 계좌인지의 여부를 판단하고, 사용금액이 약 설정금액보다 크거나 같으면 인증한다. 만약, 사용금액이 약 설정금액보다 작으면 승인한다. 그 시점에서 유자는 해당 코드데이터를 상기 금융서버(18A~18N)나 연사 서버(17)로 전송하여 카드 사용승인을 할 수 있도록 한다.

반면에, 사용금액이 약 설정금액보다 큰 경우라면, 상기 이통통신 교환기(16)는 해당 유자의 모바일 단말기(10)로 약 해제요구에 대한 SNS 데이터를 전송한다. 이에 따라, 상기 모바일 단말기(10)로부터 약 해제신호가 전송되면, 해당 약 상태를 유지하고, 승인 불가 코드데이터를 상기 금융서버(18A~18N)나 연사 서버(17)로 전송하여 카드나 계좌를 사용할 수 있도록 한다.

한편, 유자가 모바일 단말기(10)를 이용하여 약 해제에 대한 코드데이터를 발생시키면, 이통통신 교환기(16)는 해당 코드데이터를 수신하여, 해당 계좌의 사용금액에 대한 작을 해제한다. 그리고, 상기 금융서버(18A~18N)나 연사 서버(17)로 사용승인 신호를 발생시켜 해당 카드나 계좌를 사용할 수 있도록 한다.

이와, 본 발명의 제 3 실시예에 대해 도면을 참조하여 상세하게 설명한다.

도 11a, 11b는 본 발명의 제 3 실시예에 따른 계좌/금액 인증을 모바일 단말기를 이용한 금융보안 시스템을 통한 금융보안 설정화면을 도시한 도면이다.

이름 참조하면, 본 발명의 제 3 실시예에 따른 계좌/금액 인증을 모바일 단말기를 이용한 금융보안 시스템은 유자가 모바일 단말기를 이용하여 소지한 다수의 신용카드나 현금카드, 가상계좌와 관련하여 설정할 수 있는 인증/인증/인증/인증 금액을 설정할 수 있도록 이통통신 교환기(16)를 금융서버를 연계함으로써 카드 사용금액을 인증할 수 있도록 인증한 일련의 정보 사용자의 금액이나 인증금액에 설정 금액 이상 되지 않도록 한다.

즉, 커튼나 계좌의 사용여부에 대한 작을 설정하는 것과 마찬가지로, 본 발명에서는 카드나 계좌의 일일 사용한다나 인증금액을 입력로 설정하여 그 이상의 금액에 대해서는 하루에 사용할 수 있는 사용이나 인증이 불가능하도록 할 수 있는 방법을 제시한다.

이름 위해, 상기 모바일 단말기(10)는, 1. 연사 서버(17)나 연사 서버(17)에 대한 사용금액에 대한 작을 설정할 수 있는 코드데이터를 발생시킬 수 있는 프로그램으로 부가적으로 설정 사용한다나 인증금액을 설정할 수 있도록 한다. 또한, 금융서버(18A~18N)나 연사 서버(17)에서 사용한다나 인증금액을 설정할 수 있도록 한다. 즉, 인증금액에 대한 작을 인증하는 카드나 계좌의 일일 사용금액에 대한 작을 인증할 수 있도록 한다. 또한, 이 경우 설정된 금액은 신용카드사나 금융기관에서 사용자의 신용도에 따라 설정한 신용한도라는 의미이다.

한편, 본 발명의 일 실시예에 따른 인증 가능한 금액의 설정을 상기 금융서버(18A~18N)나 연사 서버(17)에서 수행하도록 할 수도 있다.

상기한 바의 절차 이후에, 시스템을 이용하여 유자는 모바일 단말기(10)를 통해 도 11a에 도시되는 화면의, 1. 비밀번호 입력, 2. 계좌 선택이나 인증, 3. 인증 가능 금액에 대한 인증 설정을 할 수 있는 화면(100)에 들어간다. 그 화면(100)에서 유자가 비밀번호를 입력하고, 특정 계좌나 카드를 선택하고, 해당 금액에 대한 인증을 입력하게 되면 해당 유자가 선택한 카드나 계좌의 일일 사용금액에 대한 작을 인증할 수 있게 된다. 또한, 이 경우 설정된 금액은 신용카드사나 금융기관에서 사용자의 신용도에 따라 설정한 신용한도라는 의미이다.

즉, 해제금액이 설정되면, 상기 이통통신 교환기(16)는 해당 유자의 모바일 단말기(10)의 유자의 계좌 ×××-×××-×××××의 일 및 약 해제금액(10만원)입니다. 이는 SNS 데이터로 공유하여 회원(100) 등록시킴다.

예를 들어, 본 발명에서는 일일 약 해제금액이 설정된 자금으로 전송되도록 하는 것이 바람직하다. 즉, 10만원의 일일 약 해제금액이 설정된 상태에서 유자가 일일 2만원만 사용하였다고, 자율 유자의 계좌는 다시 10만원의 일일 약 해제금액이 전송되면 전송되도록 하는 것이다.

10-2004-0072447

·상기인 구성의 본 발명에 제 3 실시예에 따른 계좌/금액 인증용 모바일 단말기용 미충전 금융보안 시스템의 기술적 작용을 전부일 도면을 참조하여 상세하게 설명한다.

도 12는 본 발명의 제 3 실시예에 따른 계좌/금액 인증용 모바일 단말기용 미충전 금융보안 시스템의 상호 작용을 도시한 흐름차트이다.

먼저, 유저가 그 모바일 단말기(101)를 이용하여 다수의 계좌중 적어도 하나 이상의 특정 계좌를 선택하여 꼭 설정이 가능한 계좌 인증 성공요건에 행한다. 상기 인증중인 계좌가 (16)는 해당 계좌에 대한 계좌 인증 설정을 행한다.

또한, 유저가 해당 계좌에 대한 특정 금액을 입력하여 해당 계좌의 일일 사용한도 및 인증 가능금액에 대한 막 설정을 요구하면, 상기 인증중인 계좌가 (16)는 해당 일일 사용금액에 대한 막 설정 요구에 코드대어 다음 수신하여 선택 계좌의 사용금액에 대한 막 설정한다.

그 상태에서, 해당 금융서버(18A~18H)나 뱅크 서버(17)로 ATM 연결기, 가맹점 키오스크 단말기 등을 통해 카드번호 전송이 이루어지면, 상기 금융서버(18A~18H)나 뱅크 서버(17)는 상기 인증중인 계좌가 (16)로 카드 사용 승인요건으로 및 승인금액 정보를 전송한다.

그런데, 상기 인증중인 계좌가 (16)는 해당 계좌가 막 설정된 계좌인지의 여부를 판단하고, 일단 사용금액이 막 설정금액보다 크거나 같은지를 판단한다. 만약, 일단 사용금액이 막 설정금액보다 작은 경우라면, 그 사용금액에 대한 코드대어된 상기 금융서버(18A~18H)나 뱅크 서버(17)로 전송하여 카드 사용승인을 행하도록 한다.

반면에, 사용요건 하는 금액이 일단 막 설정금액보다 큰 경우라면, 상기 인증중인 계좌가 (16)는 해당 유저 및 모바일 단말기(101)로 막 해제이후에 다음 S506 액티비티를 전송한다. 이에 따라, 상기 모바일 단말기(101)로부터 막 해제신호가 전송되면, 해당 막 해제된 유저하고, 승인 불가 코드대어되는 상기 금융서버(18A~18H)나 뱅크 서버(17)로 전송하여 커드나 계좌를 사용하지 못하도록 한다.

만약, 유저가 모바일 단말기(101)를 이용하여 막 해제에 대한 코드대어되는 발생시키면, 인증중인 계좌가 (16)는 해당 코드대어되는 수신하여, 해당 계좌의 일일 사용금액에 대한 막을 해제한다. 그리고, 상기 금융서버(18A~18H)나 뱅크 서버(17)로 사용승인 실패를 발생시켜 해당 커드나 계좌를 사용할 수 있도록 한다.

또한, 자원은 금융 사용된 금액과는 무관하게 다시 기설정된 일일 막 설정금액으로 인증중인 계좌가 (16)에 설정된 데이터가 갱신되게 한다.

만약, 본 발명의 실시예에 따른 계좌/금액 인증용 모바일 단말기용 미충전 금융보안 시스템 및 그 방법은 단지 상기인 실시예에 한정되는 것이 아니라 그 기술적 요건을 충족하지 않는 범위내에서 다양한 변형이 가능하다.

발명의 효과

상기인 바와 같이, 본 발명에 따른 계좌/금액 인증용 모바일 단말기용 미충전 금융보안 시스템 및 그 방법은 커드나 증명이나 도장을 포함하거나, 증명, 또는 카드의 유효기간제시에도 증명이나 뱅크의 승인과는 별도로 유저와 모바일 단말기에서 승인신호를 발생하도록 하여 즉석에서의 승인 이루어질 경우에만 해당 커드나 카드를 사용할 수 있도록 함으로써 완벽한 금융보안 절차를 구축할 수 있다는 장점이 있으며, 유저가 설정에 따른 일일 금액에 대해서는 막을 해제함으로써 별도의 승인없이 커드나 계좌를 사용할 수 있도록 함으로써 더욱 편리하게 이용할 수 있으며, 해당 막을 해제함으로써 승인 없이 사용할 수 있는 인증금액이 나 사용한다 금액을 감소시킬 수 있으므로 보다 안전한 금융서비스를 제공할 수 있다는 효과가 있다.

(57) 청구의 범위

청구항 1

금융서버나 뱅크 서버로 이루어진 ATM이나 가맹점 키오스크 단말기로부터 사용승인 요구신호가 발생되면, 해당 카드의 인증을 수행하여 승인신호를 발생시키도록 하는 1차 승인수단과:

상기 1차 승인수단과 더불어, 유저가 설정한 계좌나 카드를 사용여부에 대한 승인신호를 발생시키기 위해 모바일 단말기를 이용하여 구성되며, 승인 여부에 대한 S506 전송을 위해 커드나 계좌에 대한 송신 기 부속품을 발생시키는 2차 승인수단인;

상기 2차 승인수단들 통해 유저가 미리 지정한 계좌나 카드를 등록시키고, 2차 승인수단을 통해 지정한 커드나 카드의 특성값/해제설정값 할하여, 상기 1차 승인수단으로부터 커드나 계좌의 사용신호를 접수받아 막 설정된 커드나 계좌인 경우 해당 사용승인 여부에 대한 유효기간제시 S506을 2차 승인수단으로 전송하고, 그 응답 데이터를 수신하여 1차 승인수단으로 전송함으로써 계좌나 카드를 사용이 가능하도록 하는 승인 설정수단;

상기 1차 승인수단, 2차 승인수단 및 승인 설정수단의 사이에 매개한 인증통신 기지국, 인증통신 중계국, 인증통신 제어국으로 이루어진 것을 더하여서 인증신호를 양하는 데이터 송수신단으로 이루어진 것을 특징으로 하는 계좌/금액 인증용 모바일 단말기용 미충전 금융보안 시스템.

청구항 2

제 1 항에 있어서, 상기 2차 승인수단은 사용자의 선택 조작에 따라 상대방과 전화번호로 입력과, 문자메시지의 작성을 위한 문자의 입력, 카드 선택 및 그 사용승인을 위한 다양한 제능기능의 선택을 위한 다수의 기능 커비튼을 갖추고 있으며, 전송된 카드번호 승인요구에 대한 인증 메시지에 대한 선택 커비튼을 통해 인증과 해당 카드사용, 송신에 대한 코드정보를 작성하는 기능 커비튼과; 카드사용 승인에 대한 막 설정

10-2004-3072447

해당 카드나 계좌에 대한 인증을 행하는 1차 승인과정과;

해당 카드나 계좌의 2차 사용승인을 허용통신 요건기에 맞추는 과정과;

해당 카드나 계좌에 학이 설정되었는 지를 판단하는 과정과;

학이 설정된 경우, 해당 유자의 모바일 단말기로 학을 해제할 권한자에 대한 인증메시지를 전송하는 과정과;

유자가 모바일 단말기를 이용하여 해당 카드나 계좌의 학을 해제함으로써 2차 승인승인을 발생하는 과정으로 이루어진 것을 특징으로 하는 계좌/금액 인증용 모바일 단말기를 이용한 금융보안 방법.

청구항 7

제 6 항에 있어서, 상기 인증통신 요건기에서 해당 유자의 카드나 계좌에 학이 설정되지 않은 경우라면, 유자의 승인에 무관하게 자체적으로 2차 승인승인을 발생하는 과정이 더 포함될 것을 특징으로 하는 계좌/금액 인증용 모바일 단말기를 이용한 금융보안 방법.

청구항 8

제 6 항에 있어서, 유자가 모바일 단말기를 이용하여 해당 카드나 계좌의 학을 해제함으로써 2차 승인승인을 발생하는 과정이론 카드나 계좌의 비밀번호와 일치한 별도의 비밀번호를 입력하는 과정과; 학 해제된 뒤론 해당 카드나 카드를 선택하는 과정과; 학 해제 된 상태를 확인 해주는 선택하는 과정이 더 포함될 것을 특징으로 하는 계좌/금액 인증용 모바일 단말기를 이용한 금융보안 방법.

청구항 9

제 8 항에 있어서, 유자가 모바일 단말기를 이용하여 해당 카드나 계좌에서 인증/사용 가능한 금액을 확인해 주는 과정과; 금액이 지나거나 또는 서버로부터 2차 승인요구신호와 사용금액 정보가 전송되는 과정과; 해당 카드나 카드의 학이 설정되었는 지를 판단하는 과정과; 해당 사용금액이 허용정된 금액보다 많거나 요구를 판단하는 과정과; 2차 승인승인을 발생하는 과정이 더 포함될 것을 특징으로 하는 계좌/금액 인증용 모바일 단말기를 이용한 금융보안 방법.

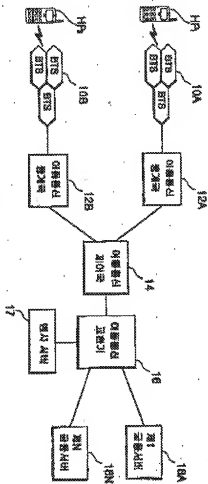
청구항 10

제 8 항에 있어서, 유자가 모바일 단말기를 이용하여 해당 카드나 계좌의 원금 금액을 설정하여 해당 금액의 사용에 대한 학을 해제하는 과정에는 일일 사용금액에 대한 학을 해제하는 과정과; 해당 일일 사용금액에 대한 학을 마칠 경신하여 해제되도록 하는 과정이 더 포함될 수 있는 것을 특징으로 하는 계좌/금액 인증용 모바일 단말기를 이용한 금융보안 방법.

10-2004-0072447

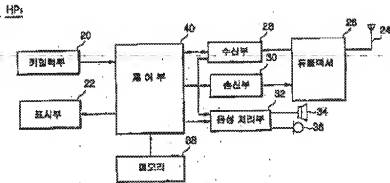
도면

1도면

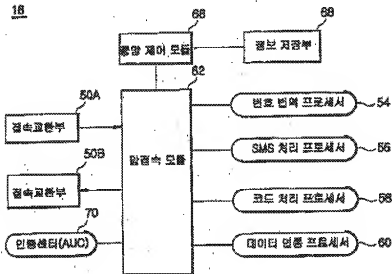


10-2004-0072447

도면2



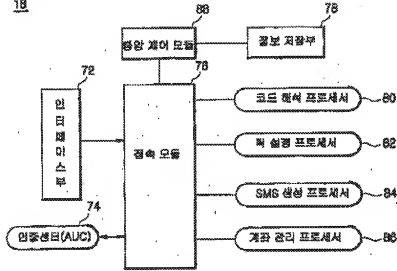
도면3



10-2004-0072447

도면4

18



도면5

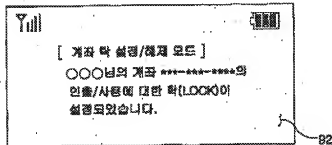
Y!!! [계좌 및 설정/결제 모드]

1. 비밀번호 입력
2. 계좌 선택
3. 계좌 및 설정
4. 계좌 및 결제

90

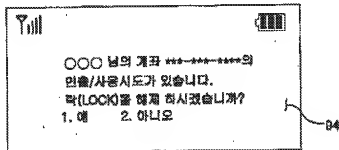
10-2004-0072447

도면5



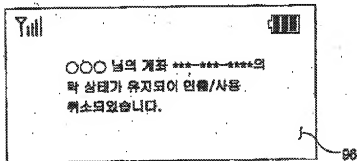
82

도면6



84

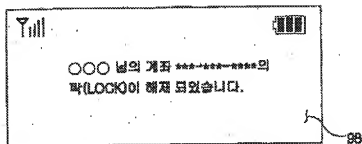
도면7



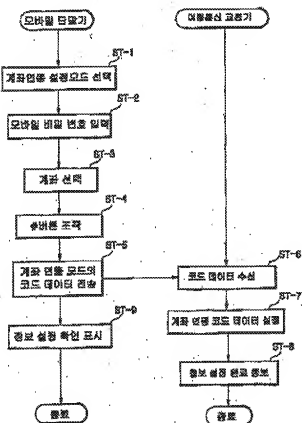
86

10-2004-0072447

도면6c



도면7



10-2004-0072447

도면명

YIII

[계좌 락 설정/해제 모드]

1. 비밀번호 입력

2. 계좌 선택

3. 락 해제 금액 설정

100

도면명

YIII

[계좌 락 설정/해제 모드]

OOO님의 계좌 -----의
잔고 (사용할도) 에서 [10] 만원이
락 해제 되었습니다.

102

10-2004-0072447

도면11a

Y!!!

[계좌 약 설정/해제 모드]

1. 비밀번호 입력

2. 계좌 선택

3. 일일 약 설정 금액 입력

104

도면11b

Y!!!

[계좌 약 설정/해제 모드]

○○○님의 계좌 ***-**-****의
일일 약 해제 한도는 만원
입니다.

106

